Journal of Number Theory **94**, 219–223 (2002)
doi:10.1006/jnth.2001.2737

On the Diophantine Equation $a^3+b^3+c^3+d^3=0$

Rachel Gar-el and Leonid Vaserstein

Department of Mathematics, Penn State University, University Park, Pennsylvania 16802
E-mail: gar-el@math.psu.edu, vstein@math.psu.edu

Communicated by D. Goss

Received September 27, 1999

INTRODUCTION

The equation

has been studied by many mathematicians since Diophantus (see [B, p. 24; C; D, pp. 550–562; S]). Partial solutions in integers and complete solutions in rational numbers have been found.

A general solution of (1) found by Euler (see [H, pp. 290–291) involves the following polynomials $s_i = s_i(x, y, z)$:

$$s_1 := 9x^3+9x^2y+3xy^2+3y^3-3x^2z+6xyz-3y^2z+3xz^2+yz^2-z^3,$$
$$s_2 := 9x^3-9x^2y+3xy^2-3y^3+3x^2z+6xyz+3y^2z+3xz^2-yz^2+z^3,$$
$$s_3 := -9x^3+9x^2y-3xy^2+3y^3+3x^2z+6xyz+3y^2z-3xz^2+yz^2+z^3,$$
$$s_4 =: -9x^3-9x^2y-3xy^2-3y^3-3x^2z+6xyz-3y^2z-3xz^2-yz^2-z^3.$$

Using these polynomials, all rational solutions to (1) can be described in the following way:

THEOREM 1. *All rational solutions* (a, b, c, d) *of* (1) *up to nonzero rational factors are in* 1–1 *correspondence with all triples* (x, y, z) *up to nonzero rational factors according to the formulas* $(x, y, z) \mapsto (a, b, c, d) = (s_1, s_2, s_3, s_4)$; *and* $(a, b, c, d) \mapsto (x, y, z) = (ac-bd, -a^2+ab-b^2+c^2-cd+d^2, a^2-ab+b^2-ac+2bc+c^2+2ad-bd-cd+d^2)$.

This theorem allows us to describe all integer solutions as follows:

0022-314X/02 $35.00

COROLLARY 2. *Up to a rational factor, every integral solution* (a, b, c, d) *of* (1) *is equal to* (s_1, s_2, s_3, s_4) *where* $s_i = s_i(x, y, z)$ *are as above with integers* x, y, z. *Every integral primitive solution* (a, b, c, d) *of* (1) *can be written uniquely as* $(s_1, s_2, s_3, s_4)/D$ *with* $D = \gcd(s_1, s_2, s_3, s_4)$ *where* s_i *are as above with integral primitive* (x, y, z).

Recall that an n-tuple $(u_1, \ldots, u_n)$ of integers is called *primitive* if $\gcd(u_1, \ldots, u_n) = 1$. Here gcd stands for the greatest common divisor which takes integral nonnegative values.

Corollary 2 does not give an explicit description of all integral primitive solutions to (1) since it is not clear from the definition $D = \gcd(s_1, s_2, s_3, s_4)$ what are possible values for D when (x, y, z) ranges over all integral primitive triples. So the complete solution of (1) in integers was pointed out as an open problem in [B, p. 10; C, p. 1251; H, p. 290; Ha, pp. 199–200; R, v.3, p. 197; S, pp. 121–122].

For comparison, let us consider a simpler Diophantine equation

$$a^2 + b^2 = c^2. \tag{2}$$

It is well known that every primitive integral solution (a, b, c) of (2) can be written as $\pm(x^2 - y^2, 2xy, x^2 + y^2)/d$ with a primitive pair (x, y) which is unique, up to sign, and

$$d = \gcd(x^2 - y^2, 2xy, x^2 + y^2).$$

The explicit description of this number d is given as follows: $d = \mathrm{mod}(x, 2) + \mathrm{mod}(y, 2)$. Here and further on, $\mathrm{mod}(x, 2)$ denotes the remainder on division of x by 2. So $d = 2$ when xy is odd, and $d = 1$ otherwise. Thus, Eq. (2) is completely solved in integers.

In this paper we address the problem of finding an explicit description of the number D in Corollary 3. Our main result is:

THEOREM 3. *Every integral primitive solution* (a, b, c, d) *of* (1) *can be written uniquely as* $(s_1, s_2, s_3, s_4)/D$ *with* $D = \gcd(s_1, s_2, s_3, s_4) = d_0 d_2 d_3$ *where polynomials* $s_i = s_i(x, y, z)$ *are as above with integral primitive* (x, y, z) *and*

$$d_0 = \gcd(x, 3y^2 + z^2)\gcd(y, 3x^2 + z^2)\gcd(z, 3x^2 + y^2),$$

$$d_2 = \begin{cases} 4 & \text{when } \mathrm{mod}(x, 2) + \mathrm{mod}(y, 2) + \mathrm{mod}(z, 2) = 2 \text{ and } \mathrm{mod}(xyz, 4) \neq 0, \\ 2 & \text{when } \mathrm{mod}(x, 2) + \mathrm{mod}(y, 2) + \mathrm{mod}(z, 2) = 2 \text{ and } \mathrm{mod}(xyz, 4) = 0, \\ 1 & \text{otherwise,} \end{cases}$$

$$d_3 = \begin{cases} 3 & \text{when } \mathrm{mod}(z, 3) = 0 \text{ and } \mathrm{mod}(xy, 3) \neq 0, \\ 1 & \text{otherwise.} \end{cases}$$

Our description of D is explicit enough to answer what its possible values are.

COROLLARY 4. *When* (x, y, z) *ranges over all primitive integral triples, the number* D *in Corollary* 2 *ranges over all numbers of the form* t_2t_3t *where* t_2 *is* 1 *or* 8, t_3 *is* 1, 3, *or* 9, *and* t *is any product of primes of the form* $3k+1$.

Note that while the number d for Eq. (2) is bounded, the number D for Eq. (1) is not. While there are many polynomial solutions for (1) with integral coefficients besides (s_1, s_2, s_3, s_4), we believe that the set of primitive integral solutions of (1) cannot be covered by a finite set of polynomial families with integral coefficients.

1. *Proof of Theorem* 3. By Theorem 1, $(s_1, s_2, s_3, s_4)=0$ if and only if $(x, y, z)=0$. Assume now that $(s_1, s_2, s_3, s_4)\neq 0$. Let $D=\gcd(s_1, s_2, s_3, s_4)$. Let p^m be a primary factor of D, i.e., p is a prime and p^m is the highest power of p dividing D.

We have to prove that p^m is equal to the highest power p^n of p dividing $d_0d_2d_3$. (By definition, D and all d_i are positive.)

Now we consider three cases:

Case 1: $p\geqslant 5$. First we prove that $m\leqslant n$, i.e., $p^m \mid d_0$. If $m=0$, there is nothing to prove, so let $m\geqslant 1$.

Since $p^m \mid s_1$, we conclude: if p divides both x and y, then $p \mid z^3$, hence p divides z; if p divides both x and z, then p divides $3y^3$; if p divides both z and y, then p divides $9x^3$. Since (x, y, z) is primitive and $p\neq 3$, p divides at most one of the numbers x, y, z.

Since p^m divides $s_1+s_2+s_3+s_4=24xyz$, we conclude that p^m divides x, y, or z.

Subcase 1x: $p\geqslant 5$ and p^m divides x. Then p^m divides

$$(s_2+s_3)|_{x=0}=2z(3y^2+z^2);$$

hence $p^m \mid 3y^2+z^2$. Therefore $p^m \mid d_0$.

Subcase 1y: $p\geqslant 5$ and p^m divides y. Then p^m divides

$$(s_2+s_3)|_{y=0}=2z(3x^2+z^2);$$

hence $p^m \mid 3x^2+z^2$. Therefore $p^m \mid d_0$.

Subcase 1z: $p\geqslant 5$ and p^m divides z. Then p^m divides

$$(s_1+s_2)|_{z=0}=6z(3x^2+y^2);$$

hence $p^m \mid 3x^2+y^2$. Therefore $p^m \mid d_0$.

Thus, $p^m \mid d_0$ in all three subcases, i.e., $m\leqslant n$ in Case 1.

Since $p^n \mid d_0$, we conclude that either p^n divides both x and $3y^2+z^2$, it divides both y and $3z^2+x^2$, or else it divides both z and $3x^2+y^2$. Therefore in all three cases it divides D, i.e., $m \geqslant n$. Thus, $m = n$ in Case 1.

Case 2: $p = 2$. When only one or all three of (x, y, z) are odd, D is odd, so $m = 0$. In this case, also all three d_0, d_2, d_3 are odd so $n = 0 = m$.

Assume now that exactly two of the numbers (x, y, z) are odd; i.e.,

$$\mathrm{mod}(x, 2)+\mathrm{mod}(y, 2)+\mathrm{mod}(z, 2) = 2.$$

Then $m=3$ and $n=3$ as well.

Case 3: $p = 3$. When $\mathrm{mod}(z, 3) \neq 0$, $m = n = 0$. When $\mathrm{mod}(z, 3) = 0$ and $\mathrm{mod}(y, 3) \neq 0$, then $m = 1$, and also $n = 1$. When $\mathrm{mod}(z, 3) = 0 = \mathrm{mod}(y, 3)$, then $m = 2$, and also $n = 2$.

2. *Proof of Corollary* 4. In the proof of Theorem 3 in Cases 2 and 3, we saw that the power of two dividing D can be 1 or 8, and the power of three dividing D can be 1, 3, or 9. Now let p be a prime $\geqslant 5$ dividing D. Modulo such a prime, -3 is a square; therefore the multiplicative group modulo p contains an element of order 3, so $p-1$ is divisible by 3; i.e., $p = 3k+1$. Therefore D has the form described in Corollary 6.

Now it remains to be proved that every number D of this form can actually occur. We write $D = 2^m 3^n d'$ where $m=0$ or 3, $n=0$, 1, or 2, and d' is a product of primes of the form $3k+1$.

We take $x = d'$. We set

$$y = \begin{cases} 1 & \text{when} \quad n \leqslant 1, \\ 3 & \text{otherwise.} \end{cases}$$

Note that -3 is a square modulo every prime of the form $3k+1$, and so is $-3y^2$. By the Chinese remainder theorem, we can choose z such that $\mathrm{mod}(z^2+3y^2, x) = 0$; i.e., $\gcd(x, 3y^2+z^2) = x = d'$. In addition, we can impose on z any congruences modulo 4 and 3. We require z to be odd when $m = 0$ and $\mathrm{mod}(z, 4) = 0$ otherwise. We require $\mathrm{mod}(z, 3) = \mathrm{mod}(D, 3)$. Still we can replace z by $z+12ux$ with any integer u keeping all these conditions intact. Since $\gcd(3x^2+y^2, 12x)$ divides 12, we can arrange that $\gcd(z, 3x^2+y^2) \mid 12$.

Then:

$$\gcd(z, 3x^2+y^2) = \begin{cases} 1 & \text{when} \quad n \leqslant 1 \quad \text{and} \quad m = 0, \\ 3 & \text{when} \quad n = 2 \quad \text{and} \quad m = 0, \\ 4 & \text{when} \quad n \leqslant 1 \quad \text{and} \quad m \geqslant 1, \\ 12 & \text{otherwise,} \end{cases}$$

$$\gcd(x, 3y^2+z^2) = d',$$

and

$$\gcd(y, 3x^2+z^2) = \begin{cases} 1 & \text{when} \quad n \leqslant 1, \\ 3 & \text{otherwise.} \end{cases}$$

Therefore $d_0 = 2^{m'}3^{n'}d'$ where

$$m' = \begin{cases} 0 & \text{when} \quad m = 0, \\ 2 & \text{when} \quad m = 3, \end{cases}$$

and

$$n' = \begin{cases} 0 & \text{when} \quad n \leqslant 1, \\ 2 & \text{when} \quad n = 2, \end{cases}$$

hence $D = d_2 d_3 d'$.

REFERENCES

[B] B. C. Berndt, Y.-S. Choi, and S.-Y. Kang, The problems submitted by Ramanujan to the Journal of the Indian Mathematical Society, *in* "Proceedings of Continued Fractions: From Analytic Number Theory to Constructive Approximation, University of Missouri May 1998" (B. C. Berndt and F. Gesztesy, Eds.), AMS Cont. Math., Vol. 236, pp. 15–56, Amer. Math. Soc., Providence, RI, 1999.

[C] A. Choudhry, On equal sums of cubes, *Rocky Mountain J. Math.* **28** (1998), 1251–1257.

[D] L. E. Dickson, "History of the Theory of Numbers, Vol. 2, Diophantine Analysis," Chelsea, New York, 1966.

[H] L.-K. Hua, "Introduction to Number Theory," Springer-Verlag, Berlin/New York, 1982.

[Ha] G. H. Hardy and E. M. Wright, "An Introduction to the Theory of Numbers," 5th ed., Clarendon Press, Oxford, Oxford Univ. Press, New York, 1979.

[R] B. C. Berndt, (Ed.), "Ramanujan's Notebooks," Springer-Verlag, New York, 1985–1998.

[S] C. Sándor, On the equation $a^3+b^3+c^3=d^3$, *Period. Math. Hungar.* **33** (1996), 121–134.